Entanglement of Subspaces and Error Correcting Codes

Gilad Gour[1,*] and Nolan R. Wallach[2,†]

[1] *Institute for Quantum Information Science and Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4*

[2] *Department of Mathematics, University of California/San Diego, La Jolla, California 92093-0112*

(Dated: February 1, 2008)

We introduce the notion of *entanglement of subspaces* as a measure that quantify the entanglement of bipartite states in a randomly selected subspace. We discuss its properties and in particular we show that for maximally entangled subspaces it is additive. Furthermore, we show that maximally entangled subspaces can play an important role in the study of quantum error correction codes. We discuss both degenerate and non-degenerate codes and show that the subspace spanned by the logical codewords of a non-degenerate code is a k-totally (maximally) entangled subspace. As for non-degenerate codes, we provide a mathematical definition in terms of subspaces and, as an example, we analyze Shor's nine qubits code in terms of 22 mutually orthogonal subspaces.

PACS numbers: 03.67.Mn, 03.67.Hk, 03.65.Ud

I. INTRODUCTION AND DEFINITIONS

Bipartite entanglement has been recognized as a crucial resource for quantum information processing tasks such as teleportation [1] and super dense coding [2]. As a result, in the last years there has been an enormous effort to understand and study the characterization, manipulation and quantification of bipartite entanglement [3]. Yet, despite a great deal of progress that was achieved, the theory on mixed bipartite entanglement is incomplete and a few central important questions such as the additivity of the entanglement of formation [4] remained open. Perhaps the richness and complexity of mixed bipartite entanglement can be found in the fact that a finite set of measures of entanglement is insufficient to completely quantify it [5]. In this paper we shed some light on mixed bipartite entanglement with the introduction of a new kind of measure of entanglement which we call entanglement of subspaces (EoS). We will see that EoS can play an important role in the study of quantum error correcting codes (QECC).

It has been shown recently [6, 7] that geometry of high-dimensional vector spaces can be counterintuitive especially when subspaces with very unique properties are more common than one intuitively expects. That is, roughly speaking, if a high dimensional subspace is selected randomly it is quite likely to have strange properties. For example, in [7] it has been demonstrated that a randomly chosen subspace of a bipartite quantum system will likely contain nothing but nearly maximally entangled states even if the dimension of the subspace is almost of the same order as the dimension of the original system. This kind of result has implications, in particular, to super-dense coding [8] and for quantum communication in general (see also [9] for other implications of randomly selected subspaces). The quantification of the entanglement of such subspaces is therefore very important and we start with its definition.

Definition 1. Let $\mathcal{H}^{\mathrm{A}}$ and $\mathcal{H}^{\mathrm{B}}$ be finite dimensional Hilbert spaces and let W^{AB} be a subspace of $\mathcal{H}^{\mathrm{A}}\otimes\mathcal{H}^{\mathrm{B}}$. The entanglement of W^{AB} is defined as:

$$\mathcal{E}\left(W^{\mathrm{AB}}\right)\equiv\min_{\psi^{\mathrm{AB}}\in W^{\mathrm{AB}}}\left\{E\left(\psi^{\mathrm{AB}}\right)\ :\ \|\psi^{\mathrm{AB}}\|=1\right\}, \quad (1)$$

where $E\left(\psi^{\mathrm{AB}}\right)$ is the entropy of entanglement of ψ^{AB}.

Note that if the subspace W^{AB} contains a product state then $\mathcal{E}(W^{\mathrm{AB}})=0$. On the other hand, if, for example, W^{AB} is orthogonal to a subspace spaned by an unextendible product basis (UPB) [11, 12] then $\mathcal{E}(W^{\mathrm{AB}})>0$.

Claim: Let $d_A=\dim\mathcal{H}^{\mathrm{A}}$ and $d_B=\dim\mathcal{H}^{\mathrm{B}}$. If $\mathcal{E}(W^{\mathrm{AB}})>0$ then

$$\dim W^{\mathrm{AB}}\leq(d_{\mathrm{A}}-1)(d_{\mathrm{B}}-1). \quad (2)$$

This claim follows from [10] and also related to the fact that the number of (bipartite) states in a UPB is at least $d_{\mathrm{A}}+d_{\mathrm{B}}-1$ [11]. Note that for two qubits (i.e. $d_A=d_B=2$) $\mathcal{E}(W^{\mathrm{AB}})$ can be greater than zero only for one dimensional subspaces.

We can use Eq. (1) to define another measure of entanglement on bipartite mixed states.

Definition 2. Let $\rho\in\mathcal{B}\left(\mathcal{H}^{\mathrm{A}}\otimes\mathcal{H}^{\mathrm{B}}\right)$ be a bipartite mixed state and let S_ρ^{AB} be the support subspace of ρ. Then, the entanglement of the support of ρ is defined as

$$E_{\mathrm{Support}}(\rho)\equiv\mathcal{E}(S_\rho^{\mathrm{AB}})\ .$$

It can be easily seen that this measure is not continuous and therefore can not be considered as a proper measure of entanglement. Nevertheless, this measure can serve as a mathematical tool to find lower bounds for other measures of entanglement that are more difficult to calculate

*Electronic address: gour@math.ucalgary.ca

†Electronic address: nwallach@ucsd.edu

especially in higher dimensions. For example, the entanglement of the support of ρ provides a lower bound for the entanglement of formation. It can be shown that in lower dimensions the bound is generally not tight. For example, for two qubits in a *mixed* state ρ, the entanglement of the support $E_{\rm Support}(\rho) = 0$ (see Eq. (2)). On the other hand, in higher dimensions the bound can be very tight [6, 7].

II. ENTANGLEMENT OF SUBSPACES

In this section we study some of the properties of EoS with a focus on additivity properties. The EoS provides a lower bound on the entanglement of formation and our interest in its additivity properties is due to one of the most important unresolved questions in quantum information, namely the additivity conjecture for the entanglement of formation. In particular, the additivity question of EoS is identical to the additivity conjecture of quantum channel output entropy [13] that has been shown to be equivalent to the additivity conjecture of entanglement of formation [4]. Thus, additivity properties of EoS can shed some light on this topic.

A. Additivity properties of the entanglement of subspaces

Here we consider the additivity properties of EoS. We start by showing that if $U^{\rm AB}$ and $V^{\rm A'B'}$ are two subspaces such that $\mathcal{E}(U^{\rm AB}) > 0$ and/or $\mathcal{E}(V^{\rm A'B'}) > 0$ then $\mathcal{E}(U^{\rm AB} \otimes V^{\rm A'B'}) > 0$.

Consider $W = \mathbb{C}^n \otimes \mathbb{C}^m$. Let e_j, $j = 1, ..., n$ be the standard basis of $\mathbb{C}^n$. We will also use the notation f_j for the standard basis of $\mathbb{C}^m$. An element of a tensor product of two vector spaces, A and B will be called a product if it is of the form $a \otimes b$ with $a \in A$ and $b \in B$.

Proposition 1. *Let $u_1, ..., u_d, v_1, ..., v_d \in W$ be such that if $x = \sum_i b_i v_i$ is a product then $x = 0$. If $z = \sum_i u_i \otimes v_i$ is a product in $(\mathbb{C}^n \otimes \mathbb{C}^n) \otimes (\mathbb{C}^m \otimes \mathbb{C}^m)$ then $z = 0$.*

Proof. We write $u_i = \sum_{j=1}^n e_j \otimes u_{ij}$ and $v_j = \sum_{j=1}^n e_j \otimes v_{ij}$. Assume that $\sum_i u_i \otimes v_i$ is a product in $(\mathbb{C}^n \otimes \mathbb{C}^n) \otimes (\mathbb{C}^m \otimes \mathbb{C}^m)$. This means that there exists $z \in \mathbb{C}^n \otimes \mathbb{C}^n$ and $w \in \mathbb{C}^m \otimes \mathbb{C}^m$ such that

$$\sum_{i,k,l} (e_k \otimes e_l) \otimes (u_{ik} \otimes v_{il}) = z \otimes w.$$

If we write out $z = \sum_{k,l} z_{kl} e_k \otimes e_l$ with $z_{kl} \in \mathbb{C}$ then we must have

$$\sum_i u_{ik} \otimes v_{il} = z_{kl} w$$

for all k, l. We now write $u_{ik} = \sum_m u_{ik}^m f_m$ and $w = \sum_m f_m \otimes w_m$. The displayed formula now implies that ($k.l, m$ fixed)

$$\sum_i u_{ik}^m v_{il} = z_{kl} w_m.$$

This implies that (with k and m fixed) we have

$$\sum_{il} u_{ik}^m e_l \otimes v_{il} = (\sum_l z_{kl} e_l) \otimes w_m.$$

Hence $\sum_i u_{ik}^m v_i$ is a product. Our assumption implies that it must be 0. Hence

$$0 = \sum_{i,k,m} u_{ik}^m e_k \otimes f_m \otimes v_i = \sum_i u_i \otimes v_i.$$

As was to be proved. □

Note that the proposition above states that if none of the decompositions of a bipartite mixed state, ρ, contain a product state, then also none of the decompositions of $\rho \otimes \sigma$ (σ is a bipartite mixed state) contain a product state. This property is related to the additivity conjecture [4] for the entanglement of formation (and other measures) and one of the main questions that we will consider here is wether the EoS is additive. That is, does

$$\mathcal{E}(U^{\rm AB} \otimes V^{\rm A'B'}) = \mathcal{E}(U^{\rm AB}) + \mathcal{E}(V^{\rm A'B'}) \, ?$$

Clearly, if the EoS were additive then the proposition above would have been a trivial consequence of that. However, we were not able to prove the additivity of EoS (in general) although for some special cases it has been tested numerically in [14] and no counter example has been found. The proposition below provides a lower bound.

Proposition 2. *Let $N = \min\{\dim U^{AB}, \ \dim V^{A'B'}\}$. Then*

$$\mathcal{E}(U^{AB}) + \mathcal{E}(V^{A'B'}) - \log N \leq \mathcal{E}\left(U^{AB} \otimes V^{A'B'}\right) . \quad (3)$$

The equation above provides a lower bound whereas the upper bound $\mathcal{E}\left(U^{\rm AB} \otimes V^{\rm A'B'}\right) \leq \mathcal{E}(U^{\rm AB}) + \mathcal{E}(V^{\rm A'B'})$ follows directly from the definition of EoS. Thus, for $N = 1$ the EoS is additive. Note also that even if N is small (e.g. $N = 2$), $\mathcal{E}(U^{\rm AB})$ and $\mathcal{E}(V^{\rm A'B'})$ can be arbitrarily large (i.e. depending on d_A and d_B but not on N).

Proof. Let χ be a normalized vector in $U^{\rm AB} \otimes V^{\rm A'B'}$. We can write χ in its Schmidt decomposition as follows:

$$\chi = \sum_i \sqrt{p_i} u_i^{\rm AB} \otimes v_i^{\rm A'B'} \ ,$$

where $\sum_i p_i = 1$ ($p_i \geq 0$) and the $u_i^{\rm AB}$'s ($v_i^{\rm A'B'}$'s) are orthonormal. Now, from the strong subadditivity of the von-Neumann entropy we have

$$S(\rho_{\rm A'}) + S(\rho_{\rm B}) \leq S(\rho_{\rm AB}) + S(\rho_{\rm AA'}) \ ,$$

where $\rho_{\rm A} \equiv {\rm Tr}_{\rm A'BB'}\chi \otimes \chi^*$, $\rho_{\rm B} \equiv {\rm Tr}_{\rm AA'B'}\chi \otimes \chi^*$, etc. Now, note that $S(\rho_{\rm AA'}) = E(\chi)$ and $S(\rho_{\rm AB}) = H(\{p_i\}) \leq \log N$, where $H(\{p_i\})$ is the Shanon entropy. Furthermore, note that

$$\rho_{\rm A'} = \sum_i p_i \omega_i \ \text{ and } \ \rho_{\rm B} = \sum_i p_i \sigma_i$$

where

$$\omega_i \equiv {\rm Tr}_{\rm B'} v_i^{\rm A'B'} \otimes v_i^{\rm A'B'*} \ \text{ and } \ \sigma_i \equiv {\rm Tr}_{\rm A} u_i^{\rm AB} \otimes u_i^{\rm AB*} \ .$$

Hence, since the von-Neumann entropy is concave we have

$$S(\rho_{\rm A'}) \geq \sum_i p_i S(\omega_i) = \sum_i p_i E(v_i^{\rm A'B'}) \geq \mathcal{E}\left(V^{\rm A'B'}\right) \ .$$

and similarly $S(\rho_{\rm B}) \geq \mathcal{E}\left(U^{\rm AB}\right)$. Combining all this we get

$$\mathcal{E}\left(V^{\rm A'B'}\right) + \mathcal{E}\left(U^{\rm AB}\right) \leq \log N + E(\chi) \ ,$$

for all $\chi \in U^{\rm AB} \otimes V^{\rm A'B'}$. This complete the proof. □

B. Maximally entangled subspaces

As we have seen above, if $N = 1$ then the EoS is clearly additive. As we will see in the next subsection, it is also additive for maximally entangled subspaces:

Definition 3. Let W be a subspace of $\mathcal{H}^{\rm A} \otimes \mathcal{H}^{\rm B}$ and let $d_{\rm A} = \dim \mathcal{H}^{\rm A}$ and $d_{\rm B} = \dim \mathcal{H}^{\rm B}$. W is said to be a maximally entangled subspace in $\mathcal{H}^{\rm A} \otimes \mathcal{H}^{\rm B}$ if

$$\mathcal{E}(W) = \log m \ , \tag{4}$$

where $m \equiv \min\{d_{\rm A},\ d_{\rm B}\}$.

The term maximally entangled subspace have been used in [6, 7] for a subspace W with $\mathcal{E}(W)$ slightly less than $\log m$. In this paper, we will call such subspaces nearly maximally entangled to distinguish from (exactly) maximally entangled subspaces as defined above.

In [15] it has been shown that the average entanglement of a pure state $\phi \in \mathcal{H}^{\rm A} \otimes \mathcal{H}^{\rm B}$ which is chosen randomly according to the unitarily invariant measure satisfies

$$\langle E(\phi) \rangle \geq \log_2 d_{\rm A} - \frac{d_{\rm A}}{2 \ln 2 d_{\rm B}}$$

where without loss of generality $d_{\rm A} \geq d_{\rm B}$. Later on, in [6, 7] this result has been extended to subspaces and in particular it has been shown, somewhat surprisingly, that a randomly chosen subspace of bipartite quantum system will likely be a nearly maximally entangled subspace. Thus, as nearly maximally entangled subspaces are quite common it is important to understand their structure. As a first step in this direction, in the following we study the structure of (exactly) maximally entangled subspaces.

Let ϕ be a state in $\mathcal{H}^{\rm A} \otimes \mathcal{H}^{\rm B}$. If $e_1, ..., e_m$ is an orthonormal basis of $\mathcal{H}^{\rm B}$ we may write

$$\phi = \sum_{i=1}^{d_B} \phi_i \otimes e_i \ .$$

We define a $d_{\rm B} \times d_{\rm B}$ Hermitian matrix $B = [\langle \phi_i | \phi_j \rangle]$ (i.e. B is the reduced density matrix). Let $\lambda_1, ..., \lambda_{d_{\rm B}}$ be the set of eigenvalues of B counting multiplicity. Then the entanglement of ϕ is

$$E(\phi) = -\sum_i \lambda_i \log(\lambda_i) \ .$$

It is easy to show that $E(\phi) \leq \log m$ and equality is attained if and only if $B = \frac{1}{m} P$ with P a projection matrix onto a d dimensional subspace of $\mathbb{C}^{d_{\rm B}}$. Clearly this definition of entropy is independent of the choice of basis and could also be given using an orthonormal basis of $\mathcal{H}^{\rm A}$ and analyzing the corresponding $d_{\rm A}$ coefficients in $\mathcal{H}^{\rm B}$. Under the condition of equality ϕ is maximally entangled, and this in particular implies that if $d_{\rm A} \geq d_{\rm B}$ then

$$\langle \phi_i | \phi_j \rangle = \frac{1}{d_{\rm B}} \delta_{ij}.$$

Proposition 3. *Assume that $d_A \geq d_B$ and set $m = d_B$. Let U^{AB} be a maximally entangled subspace in $\mathcal{H}^A \otimes \mathcal{H}^B$ of dimension d. If $e_1, ..., e_m$ is an orthonormal basis of $\mathcal{H}^B$ then there exist $U_1, ..., U_m$ subspaces of $\mathcal{H}^A$ such that $\langle U_i | U_j \rangle = 0$ if $i \neq j$, $\dim U_j = d > 0$ for all $j = 1, ..., m$ and unitary operators $T_i : \mathbb{C}^d \to U_i$ $i = 1, ..., m$ such that*

$$U^{AB} = \{\sum_i T_i w \otimes e_i | w \in \mathbb{C}^d\}.$$

Conversely, if $U_1, ..., U_m$ are mutually orthogonal subspaces of $\mathcal{H}^A$ such that $\dim U_j = d > 0$ for all $j = 1, ..., m$ and we have unitary operators $T_i : \mathbb{C}^d \to U_i$ $i = 1, ..., m$ such that

$$U^{AB} = \{\sum_i T_i w \otimes e_i | w \in \mathbb{C}^d\} \ ,$$

then U^{AB} is maximally entangled.

Proof. Let $\psi_1, ..., \psi_d$ be an orthonomal basis of $U^{\rm AB}$. Then we can write

$$\psi_j = \sum_i \psi_{ij} \otimes e_i$$

with $\langle \psi_{ij} | \psi_{kj} \rangle = \frac{1}{m} \delta_{ik}$. The condition on $U^{\rm AB}$ is that if $a \in \mathbb{C}^d$ is a unit vector then $\sum a_j \psi_j$ is maximally entangled in $\mathcal{H}^{\rm A} \otimes \mathcal{H}^{\rm B}$. This implies that

$$\left\langle \sum_{j=1}^d a_j \psi_{lj} \middle| \sum_{j=1}^d a_j \psi_{kj} \right\rangle = \frac{1}{m} \delta_{l,k} \ .$$

Fix $l \neq k$ and let $p \neq q \leq d$ be two integers. Let $a = (a_1, ..., a_d)$ with $a_j = 0$ for $j \neq p$ or $j \neq q$. Set $a_p = b, a_q = c$ and $|b|^2 + |c|^2 = 1$. Then we have

$$\langle b\psi_{lp} + c\psi_{lq} | b\psi_{kp} + c\psi_{kq} \rangle = 0.$$

On the other hand we have

$$\langle b\psi_{lp} + c\psi_{lq} | b\psi_{kp} + c\psi_{kq} \rangle = \overline{b}c \langle \psi_{lp} | \psi_{kq} \rangle + \overline{c}b \langle \psi_{lq} | \psi_{kp} \rangle$$

Set $z = \overline{b}c$. We look at two cases: first $z = \frac{1}{2}$ ($b = c = \frac{1}{\sqrt{2}}$) and second $z = \frac{i}{\sqrt{2}}$ ($b = \frac{1}{\sqrt{2}}, c = \frac{i}{\sqrt{2}}$). Thus we have

$$\langle \psi_{lp} | \psi_{kq} \rangle + \langle \psi_{lq} | \psi_{kp} \rangle = 0$$

for the first case and

$$\langle \psi_{lp} | \psi_{kq} \rangle - \langle \psi_{lq} | \psi_{kp} \rangle = 0$$

for the second. Hence, $\langle \psi_{lp} | \psi_{kq} \rangle = \langle \psi_{lq} | \psi_{kp} \rangle = 0$. We set $U_l = \mathrm{Span}\{\psi_{lp} | p = 1, ..., d\}$. Then $\langle U_l | U_k \rangle = 0$ if $l \neq k$. We now consider what happens when $l = k$. We first note that taking $a_p = 1$ and all other entries equal to 0 we have $\langle \psi_{lp} | \psi_{lp} \rangle = \frac{1}{m}$. Now using b, c as above for $p \neq q$ we have

$$\langle \psi_{lp} | \psi_{lp} \rangle + \langle \psi_{lp} | \psi_{lq} \rangle + \langle \psi_{lq} | \psi_{lp} \rangle + \langle \psi_{kp} | \psi_{kp} \rangle = \frac{2}{m}$$

and

$$\langle \psi_{lp} | \psi_{lp} \rangle + i \langle \psi_{lp} | \psi_{lq} \rangle - i \langle \psi_{lq} | \psi_{lp} \rangle + \langle \psi_{kp} | \psi_{kp} \rangle = \frac{2}{m}.$$

Hence as above we find that $\langle \psi_{lp} | \psi_{lq} \rangle = 0$ if $p \neq q$. Thus $\sqrt{m}\psi_{l1}, ..., \sqrt{m}\psi_{ld}$ is an orthonormal basis of U_l. This implies that the spaces $U_1, ..., U_m$ have the desired properties. Let $u_1, ..., u_d$, be the standard orthonormal basis of $\mathbb{C}^d$ and define $T_i u_j = \sqrt{m}\psi_{ij}$. With this notation in place U^{AB} has the desired form. The converse is proved by the obvious calculation. □

Corollary 4. *If U^{AB} is a maximally entangled subspace in $\mathcal{H}^A \otimes \mathcal{H}^B$ ($d_A \geq d_B$), then*

$$\dim U^{AB} \leq \left\lfloor \frac{d_A}{d_B} \right\rfloor .$$

Furthermore, there always exists a maximally entangled subspace of dimension $\lfloor d_A/d_B \rfloor$.

Proof. Assume that $\dim \mathcal{H}^{\mathrm{A}} = d_{\mathrm{A}} \geq \dim \mathcal{H}^{\mathrm{B}} = d_{\mathrm{B}}$. According to the first part of Proposition 4, if U^{AB} is a maximally entangled subspace of dimension d then $d \times d_{\mathrm{B}} \leq d_{\mathrm{A}}$. On the other hand, if $d \leq \lfloor d_{\mathrm{A}}/d_{\mathrm{B}} \rfloor$ then the second half of the statement implies that there is a maximally entangled subspace of dimension d. □

In the following we find necessary and sufficient conditions for a subspace to be maximally entangled. In section III we use this to show that maximally entangled subspaces can play an important role in the study of error correcting codes. As above we consider the space $\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{B}}$ with $\dim \mathcal{H}^{\mathrm{A}} = d_{\mathrm{A}} \geq \dim \mathcal{H}^{\mathrm{B}} = d_{\mathrm{B}}$ and a maximally entangled subspace $U^{\mathrm{AB}} \subset \mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{B}}$. We will also consider $\mathrm{End}(\mathcal{H}^{\mathrm{B}})$ to be a Hilbert space with inner product $\langle X | Y \rangle = \mathrm{Tr}(X^\dagger Y)$ for any two operators X and Y in $\mathrm{End}(\mathcal{H}^{\mathrm{B}})$.

Proposition 5. *Let $U^{AB} \subset \mathcal{H}^A \otimes \mathcal{H}^B$ be a subspace and $d_A \geq d_B$. Then, U^{AB} is maximally entangled if and only if the map $End(H^B) \otimes U^{AB} \to \mathcal{H}^A \otimes \mathcal{H}^B$ given by $X \otimes u \mapsto \sqrt{d_B}(I \otimes X)u$ is an isometry onto its image.*

Proof. Let $d = \dim U^{\mathrm{AB}}$ and let the notation be as in Proposition 3. Thus, if U^{AB} is maximally entangled and if $e_1, ..., e_{d_{\mathrm{B}}}$ is an orthonormal basis of $\mathcal{H}^{\mathrm{B}}$ then an element of U^{AB} is of the form

$$T(w) = \sum_{i=1}^{d_{\mathrm{B}}} T_i(w) \otimes e_i \ ,$$

with T_i a unitary operator from $\mathbb{C}^d$ onto a subspace U_i of $\mathcal{H}^{\mathrm{A}}$ and U_i and U_j are orthogonal for all $i \neq j$. We now calculate

$$\langle (I \otimes X)T(w) | (I \otimes Y)T(z) \rangle = \sum_{i,j} \langle T_i(w) | T_j(z) \rangle \ \langle Xe_i | Ye_j \rangle \ .$$

Now, since $\langle T_i(w) | T_j(z) \rangle = \delta_{ij} \langle w | z \rangle$ (see Proposition 3) we have:

$$\begin{aligned} \langle (I \otimes X)T(w) | (I \otimes Y)T(z) \rangle &= \sum_{i,j} \delta_{ij} \langle w | z \rangle \ \langle Xe_i | Ye_j \rangle \\ &= \langle w | z \rangle \mathrm{Tr}(X^\dagger Y) \ . \end{aligned}$$

That is, we proved that if U^{AB} is maximally entangled then the map is an isometry. For the converse we note that we have an isometry of $\mathbb{C}^d$ onto U^{AB} given by

$$T(w) = \sum_{i=1}^{d_{\mathrm{B}}} T_i(w) \otimes e_i \ .$$

Now, if the map defined in the proposition is an isometry then

$$\langle (I \otimes X)T(w) | (I \otimes Y)T(z) \rangle = \langle w | z \rangle \mathrm{Tr}(X^\dagger Y) \ .$$

That is,

$$\sum_{i,j} \langle T_i(w) | T_j(z) \rangle \ \langle Xe_i | Ye_j \rangle = \langle w | z \rangle \mathrm{Tr}(X^\dagger Y) \ ,$$

for all $X, Y \in \mathrm{End}(\mathcal{H}^{\mathrm{B}})$. Hence, we must have $\langle T_i(w) | T_j(z) \rangle = \delta_{ij} \langle w | z \rangle /$ and from Proposition 3 the subspace U^{AB} is maximally entangled. □

C. Additivity of maximally entangled subspaces

We now discuss the additivity properties of maximally entangled subspaces.

Proposition 6. *Let $U^{AB} \subset \mathcal{H}^A \otimes \mathcal{H}^B$ and $V^{A'B'} \subset \mathcal{H}^{A'} \otimes \mathcal{H}^{B'}$ be maximally entangled subspaces. Then,*

$$\mathcal{E}\left(U^{AB} \otimes V^{A'B'}\right) = \mathcal{E}\left(U^{AB}\right) + \mathcal{E}\left(V^{A'B'}\right) = \log m + \log m' \,, \tag{5}$$

where $m \equiv \min\{d_A,\ d_B\}$ and $m' \equiv \min\{d_{A'},\ d_{B'}\}$.

Remark. From the above proposition it follows that if $d_A \geq d_B$ and $d_{\mathrm{A}'} \geq d_{\mathrm{B}'}$ or $d_B \geq d_A$ and $d_{\mathrm{B}'} \geq d_{\mathrm{A}'}$ then $U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}$ is maximally entangled in $(\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{A}'}) \otimes (\mathcal{H}^{\mathrm{B}} \otimes \mathcal{H}^{\mathrm{B}'})$. However, if for example $d_A > d_B$ and $d_{\mathrm{A}'} < d_{\mathrm{B}'}$ then $U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}$ is NOT maximally entangled in $(\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{A}'}) \otimes (\mathcal{H}^{\mathrm{B}} \otimes \mathcal{H}^{\mathrm{B}'})$ because $mm' < \min\{d_{\mathrm{A}} d_{\mathrm{A}'},\ d_{\mathrm{B}} d_{\mathrm{B}'}\}$.

Proof. There are basically two possibilities (up to interchanging factors): the first is $d_A \geq d_B$ and $d_{\mathrm{A}'} \geq d_{\mathrm{B}'}$, and the second is $d_A \geq d_B$ and $d_{\mathrm{A}'} < d_{\mathrm{B}'}$.

In the first case we have as in the statement of proposition 3 the subspaces U_j and the unitaries $T_j : \mathbb{C}^d \to U_j$ such that $U^{\mathrm{AB}} = \{\sum_i T_i w \otimes e_i | w \in \mathbb{C}^d\}$. We also have the orthonormal basis f_i of $\mathcal{H}^{\mathrm{B}'}$, the subspaces V_j and the unitaries $S_j : \mathbb{C}^{d'} \to V_j$ such that $V^{\mathrm{A'B'}} = \{\sum_i S_i w' \otimes f_i | w' \in \mathbb{C}^{d'}\}$. Thus, as a subspace of $(\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{A}'}) \otimes (\mathcal{H}^{\mathrm{B}} \otimes \mathcal{H}^{\mathrm{B}'})$, $U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}$ is spanned by the elements

$$\sum_{i,j} (T_i w \otimes S_j w') \otimes (e_i \otimes f_j).$$

Thus if we identify $\mathbb{C}^d \otimes \mathbb{C}^{d'}$ with $\mathbb{C}^{dd'}$ then the converse assertion in proposition 3 implies that $U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}$ is a maximally entangled space. This implies that

$$\mathcal{E}\left(U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}\right) = \log d_{\mathrm{B}} + \log d_{\mathrm{B}'} = \log m + \log m' \,.$$

We now consider the second case. For U^{AB} we have exactly as above $U^{\mathrm{AB}} = \{\sum_i T_i w \otimes e_i | w \in \mathbb{C}^d\}$. For $V^{\mathrm{A'B'}}$ we denote by f_j an orthonormal basis of $\mathcal{H}^{\mathrm{A}'}$ (not of $\mathcal{H}^{\mathrm{B}'}$ as above). Thus, according to proposition 3 we have $V^{\mathrm{A'B'}} = \{\sum_i f_i \otimes S_i w' | w' \in \mathbb{C}^{d'}\}$. As a subspace of $(\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{A}'}) \otimes (\mathcal{H}^{\mathrm{B}} \otimes \mathcal{H}^{\mathrm{B}'})$, $U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}$ is spanned by the elements

$$\sum_{i,j} (T_i w \otimes f_j) \otimes (e_i \otimes S_j w').$$

We will assume first that $d' \leq d$. Let $w'_1, ..., w'_{d'}$ be an orthonormal basis of $\mathbb{C}^{d'}$. Thus, if ϕ is a state in $U^{\mathrm{AB}} \otimes V^{\mathrm{A'B'}}$ we can write it as

$$\phi = \sum_{i,j,k} (T_i w_k \otimes f_j) \otimes (e_i \otimes S_j w'_k) \,,$$

where w_k are some non-normalized vectors in $\mathbb{C}^d$. Furthermore,

$$\langle \phi | \phi \rangle = d_{\mathrm{B}} d_{\mathrm{A}'} \sum_k \|u_k\|^2 \,.$$

Hence, if ϕ is normalized then

$$\sum_k \|u_k\|^2 = \frac{1}{d_{\mathrm{B}} d_{\mathrm{A}'}} \,.$$

Now, since $S_j w'_k$ is an orthonormal set of vectors for all j and k (see proposition 3), the entanglement of ϕ as an element of $(\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{A}'}) \otimes (\mathcal{H}^{\mathrm{B}} \otimes \mathcal{H}^{\mathrm{B}'})$ is given by

$$d_{\mathrm{B}} d_{\mathrm{A}'} S(B)$$

where $B = [\langle w_i | w_j \rangle]_{1 \leq i,j \leq d'}$, and if $\lambda_1, ..., \lambda_{d'}$ are the eigenvalues of B then the von-Neumann entropy of B is

$$S(B) = -\sum \lambda_i \log \lambda_i \,.$$

Now B is the most general $d' \times d'$ self adjoint, positive semidefinate matrix with trace $1/d_{\mathrm{B}} d_{\mathrm{A}'}$. The minimum of the entropy for such matrices is

$$\frac{\log(d_a d_B)}{d_a d_B}.$$

This proves the proposition for the case $d' \leq d$. If $d < d'$ then we can prove the proposition by using the same argument, this time with w_k an orthonormal basis of $\mathbb{C}^d$ and with $B' = \left[\langle w'_i | w'_j \rangle\right]_{1 \leq i,j \leq d}$. This completes the proof. □

The above proposition also shows that the entanglement of formation is additive for bipartite states with maximally entangled support. If ρ is a mixed state in $\mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{B}}$ then the entanglement of formation is defined in terms of the convex roof extension:

$$E_{\mathrm{F}}(\rho) = \min \sum p_i E(\phi_i)$$

where the minimum taken over all decompositions

$$\rho = \sum p_i \phi_i \otimes \phi_i^*$$

with ϕ_i a pure bipartite state and $p_i > 0$ and $\sum p_i = 1$.

Corollary 7. *Let ρ and σ be mixed states in $\mathcal{B}(\mathcal{H}^A \otimes \mathcal{H}^B)$ and $\mathcal{B}(\mathcal{H}^{A'} \otimes \mathcal{H}^{B'})$, respectively. If the support subspaces S_ρ and S_σ are maximally entangled then*

$$E_F(\rho \otimes \sigma) = E_F(\rho) + E_F(\sigma) \,.$$

The proof of this corollary follows directly from the fact that for states with maximally entangled support $E_{\mathrm{F}}(\rho) = \mathcal{E}(S_\rho)$. Note that the class of mixed states with maximally entangled support is extremely small (i.e. of measure zero). In particular, it is a much smaller class than the one found by Vidal, Dur and Cirac [16] .

III. ERROR CORRECTING CODES

A. Definitions

We consider error correcting codes that are used to encode l qubits in $n \geq l$ qubits in such a way that they can correct errors on any subset of k or fewer qubits. These codes, which we call (n, l, k) error correcting codes, can be classified into two classes (for example see [17]): degenerate and non-degenerate (or orthogonal) codes. We start with a general definition of error correcting codes that is equivalent to the definition given (for example) in [17] , but here we define the codes in terms of subspaces.

Definition 4. Let $X \in End(\otimes^k \mathbb{C}^2)$ and $0 \leq i_0 < i_1 < ... < i_{k-1} \leq n-1$. The operator $X_{i_0 i_1 \cdots i_{k-1}}$ on $\otimes^n \mathbb{C}^2$, that represents the errors on the k qubits $i_1, ..., i_{k-1}$, is defined by $X_{i_0 \ldots i_{k-1}} v = \sigma(X \otimes I)\sigma^{-1} v$, where (a) $\sigma \in S_n$ (acting on $\{0, 1, ..., n-1\}$ by permutations) is defined such that $\sigma(j) = i_j$, (b) σ can act on $\otimes^n \mathbb{C}^2$ by $\sigma(v_0 \otimes v_1 \otimes \cdots \otimes v_{n-1}) = v_{\sigma(0)} \otimes v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n-1)}$ and (c) $\otimes^n \mathbb{C}^2$ is viewed as $(\otimes^k \mathbb{C}^2) \otimes (\otimes^{n-k} \mathbb{C}^2)$ (putting together the k tensor factors that correspond to the k qubits $i_1, ..., i_{k-1}$ and the rest $n-k$ tensor factors). An (n, l, k) error correcting code is defined from its following ingredients:

I. An isometry $T : \otimes^l \mathbb{C}^2 \to \otimes^n \mathbb{C}^2$.

II. Let $V_0 = T(\otimes^l \mathbb{C}^2)$. There are $V_1, ..., V_d$ mutually orthogonal subspaces of $\otimes^n \mathbb{C}^2$ that are also orthogonal to V_0.

III. For each V_j there is a unitary isomorphism, U_j, of V_j onto V_0 with $U_0 = I$.

IV. $X_{i_0 i_1 \cdots i_{k-1}} V_0 \subset \oplus_{j=0}^d V_j$.

V. Let P_j be the ortogonal projection of $\otimes^n \mathbb{C}^2$ onto V_j then if $v \in V_0$ is a unit vector and $P_j(X_{i_0 i_1 \cdots i_{k-1}} v) \neq 0$ then

$$U_j \frac{P_j(X_{i_0 i_1 \cdots i_{k-1}} v)}{\left\| P_j(X_{i_0 i_1 \cdots i_{k-1}} v) \right\|}$$

equals v up to a phase.

In the next subsection we study Shor's $(9, 1, 1)$ error correcting code and show that it satisfies this definition. However, before that, let us introduce the notion of k-*totally entangled* subspaces which will play an important role in our discussion of QECC.

Definition 5. Let $\mathcal{H}$ be the space of n qubits, $\otimes^n \mathbb{C}^2$. Corresponding to any choice of k qubits (tensor factors) we can consider $\mathcal{H} = \mathcal{H}^{\mathrm{A}} \otimes \mathcal{H}^{\mathrm{B}}$ with $\mathcal{H}^{\mathrm{A}} = \otimes^{n-k} \mathbb{C}^2$ and $\mathcal{H}^{\mathrm{B}} = \otimes^k \mathbb{C}^2$. For $k \leq n/2$ we will say that a subspace, V, of $\mathcal{H}$ is k-*totally entangled* if it is maximally entangled relative to every decomposition of $\mathcal{H}$ as above.

It is interesting to note that all the subspaces spanned by the logical codewords of the different non-degenerate error correcting codes given in [18, 19, 20] are 2-totally entangled subspaces. On the other hand, the subspaces spanned by the logical codewords of degenerate codes, like Shor's 9 qubits code, are in general only partially maximally entangled subspaces (i.e. maximally entangled for some choices of k qubits but not for all choices). In the following subsections we will see the reason for that.

B. Analysis of Shor's 9 qubits code

We start with the following notations. We set $u_\pm = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)$ so that the two logical codewords in Shor's 9 qubit code are $v_+ = u_+ \otimes u_+ \otimes u_+$ and $v_- = u_- \otimes u_- \otimes u_-$. The subspace spanned by these codewords is denoted by $V_0 = \mathbb{C}v_+ \oplus \mathbb{C}v_-$. We also denote $u_\pm^0 = (|100\rangle \pm |011\rangle)/\sqrt{2}$, $u_\pm^1 = (|010\rangle \pm |101\rangle)/\sqrt{2}$ and $u_\pm^2 = (|001\rangle \pm |110\rangle)/\sqrt{2}$.

Using these notations, we define 21 mutually orthogonal 2 dimensional subspaces orthogonal to V_0:

$V_1 = \mathbb{C}u_- \otimes u_+ \otimes u_+ \oplus \mathbb{C}u_+ \otimes u_- \otimes u_-$,
$V_2 = \mathbb{C}u_+ \otimes u_- \otimes u_+ \oplus \mathbb{C}u_- \otimes u_+ \otimes u_-$,
$V_3 = \mathbb{C}u_+ \otimes u_+ \otimes u_- \oplus \mathbb{C}u_- \otimes u_- \otimes u_+$,
$V_{4+i} = \mathbb{C}u_+^i \otimes u_+ \otimes u_+ \oplus \mathbb{C}u_-^i \otimes u_- \otimes u_-$, for $i = 0, 1, 2$,
$V_{7+i} = \mathbb{C}u_+ \otimes u_+^i \otimes u_+ \oplus \mathbb{C}u_- \otimes u_-^i \otimes u_-$, for $i = 0, 1, 2$,
$V_{10+i} = \mathbb{C}u_+ \otimes u_+ \otimes u_+^i \oplus \mathbb{C}u_- \otimes u_- \otimes u_-^i$, for $i = 0, 1, 2$,
$V_{13+i} = \mathbb{C}u_-^i \otimes u_+ \otimes u_+ \oplus \mathbb{C}u_+^i \otimes u_- \otimes u_-$, for $i = 0, 1, 2$,
$V_{16+i} = \mathbb{C}u_+ \otimes u_-^i \otimes u_+ \oplus \mathbb{C}u_- \otimes u_+^i \otimes u_-$, for $i = 0, 1, 2$,
$V_{19+i} = \mathbb{C}u_+ \otimes u_+ \otimes u_-^i \oplus \mathbb{C}u_- \otimes u_- \otimes u_+^i$, for $i = 0, 1, 2$.

If $X \in End(\mathbb{C}^2)$ (linear maps of $\mathbb{C}^2$ to $\mathbb{C}^2$) then we denote by X_i the linear map of $\otimes^9 \mathbb{C}^2$ to itself that is the tensor product of the identity of $\mathbb{C}^2$ in every tensor factor but the i-th and is X in the i-th factor thus

$$X_0 = X \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I,$$

$$X_1 = I \otimes X \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$$

etc.

Then we have (here $\lfloor x \rfloor = \max\{m | m \leq x, m \in \mathbb{Z}\}$)

$$X_i V_0 \subset V_0 \oplus V_{\lfloor i/3 \rfloor + 1} \oplus V_{i+4} \oplus V_{i+13}, 0 \leq i \leq 8.$$

We choose an observable R with

$$R_{|V_i} = \lambda_i I, 0 \leq i \leq 21$$

and

$$R_{|W} = \mu I,$$

where W is the orthogonal complement of $\oplus_{i=0}^{21} V_i$ and $\lambda_i \neq \lambda_j$ for $i \neq j$ and $\lambda_i \neq \mu$ for any i. We define a unitary operator $U_j : V_j \to V_0$ as follows: we denote the Pauli matrices by

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix},$$

and then define $U_0 = I$, $U_i = (A_1)_{3i-1}$, for $i = 1, 2, 3$, $U_i = (A_2)_{i-4}$, for $4 \leq i \leq 12$ and $U_i = (A_3)_{i-13}$, for $13 \leq i \leq 21$. This gives an one qubit error correcting code since if $v \in V_0$ is a state and if we have an error in the i-th position then we will have

$$X_i v \in V_0 \oplus V_{\lfloor i/3 \rfloor + 1} \oplus V_{i+4} \oplus V_{i+13} \ .$$

Thus, if we measure the observable R on $X_i v$ then the measurement will yield one of λ_j with $j = 0, \lfloor i/3 \rfloor + 1, i+4$ or $i + 13$ and $X_i v$ will have collapsed up to a phase to $U_j v$; hence applying U_j will fix the error.

Remark. Note that the subspace V_0 is *not* 2-totally entangled subspace. Nevertheless, V_0 has very special properties. In particular, if we group the 9 qubits as $(1, 2, 3) : (4, 5, 6) : (7, 8, 9)$, then for any choice of 2 qubits that are not from the same group, the subspace V_0 is maximally entangled with respect to the decomposition between the 2 qubits and the rest 7 qubits. If the 2 qubits are chosen from the same group then the entanglement of V_0 with respect to this decomposition is $1ebit$. Thus, out of the 36 different decompositions, with respect to 27 of them $\mathcal{E}(V_0) = 2ebits$ and with respect to the other 9 decompositions $\mathcal{E}(V_0) = 1ebit$.

C. Orthogonal codes

We now consider a somewhat more intuitive class of codes known as non-degenerate codes which we also name as orthogonal codes.

Definition 6. Let $A_0 = I, A_1, A_2, A_3$ the Pauli basis and define $A^{j_0 j_1 \cdots j_{k-1}}_{i_0 i_1 \cdots i_{k-1}}$ to be

$$(A_{j_0} \otimes A_{j_1} \otimes \cdots \otimes A_{j_{k-1}})_{i_0 \cdots i_{k-1}},$$

where $0 \leq j_r \leq 3$ and $0 \leq i_0 < i_1 < ... < i_{k-1} \leq n - 1$. Let Σ be the set of distinct operators of the form $A^{j_0 j_1 \cdots j_{k-1}}_{i_0 i_1 \cdots i_{k-1}}$. Then an orthogonal (n, l, k) code is an (n, l, k) error correcting code such that if we label Σ as the set of $d + 1$ operators $S_0 = I, S_1, ..., S_d$ then $V_j = S_j V_0$.

Note that Σ has

$$d + 1 = \sum_{r=0}^{k} 3^r \binom{n}{r}$$

elements. Thus, a necessary condition that there exist an (n, l, k) code is the quantum Hamming bound [17]:

$$\sum_{r=0}^{k} 3^r \binom{n}{r} \leq 2^{n-l}.$$

Proposition 8. *A 2^l dimensional subspace V of $\otimes^n \mathbb{C}^2$ is the V_0 of an (n, l, k)-orthoganal error correcting code if and only if V is $2k$-totally entangled.*

Proof. Let V be a $2k$-totally entangled subspace in $\mathcal{H} = \otimes^n \mathbb{C}^2$, and let $X : \otimes^k \mathbb{C}^2 \to \otimes^k \mathbb{C}^2$ be a linear map on k qubits. As above, for any $i_0 < i_1 < ... < i_{k-1}$ $(1 \leq i_l \leq n)$ we denote by $X_{i_0 i_1 ... i_{k-1}}$ the operation X on $\mathcal{H}$, when acting on the k qubits $i_0, i_1, ..., i_{k-1}$ (the rest of the $n - k$ qubits are left "untouched"). Let also $\mathcal{Z} \equiv \{X \in \text{End}\left(\otimes^k \mathbb{C}^2\right) | \text{Tr} X = 0\}$ and for any $i_0 < ... < i_{k-1}$ let $U_{i_0 ... i_{k-1}} \equiv \{X_{i_0 ... i_{k-1}} V | X \in \mathcal{Z}\}$. We define the subspace

$$\mathcal{W} = V + \sum_{i_0 < ... < i_{k-1}} U_{i_0 ... i_{k-1}} \ .$$

That is, $\mathcal{W}$ consists of all the possible states after an error on k or less qubits has been occurred. Now, let $A_0 = I, \ A_1, \ A_2, \ A_3$ be an orthonormal basis of $\text{End}(\mathbb{C}^2)$ with A_i invertible (e.g. the Pauli basis of 2×2 matrices). As in Definition 6, we denote by $A^{j_0 ... j_{k-1}}_{i_0 ... i_{k-1}}$ the operator $X_{i_0 ... i_{k-1}}$ that corresponds to $X = A_{j_0} \otimes \cdots \otimes A_{j_{k-1}}$, and the set of all such operators we denote by

$$\Sigma \equiv \{A^{j_0 ... j_{k-1}}_{i_0 ... i_{k-1}} | 1 \leq i_l \leq n, \ 0 \leq j_l \leq 3\} \ .$$

Now, let $v_1, ..., v_d$ be an orthonormal basis of V and define

$$\mathfrak{B} \equiv \{S v_i \Big| S \in \Sigma, \ 1 \leq i \leq d\}.$$

We now argue that $\mathfrak{B}$ is an orthonormal basis of $\mathcal{W}$. Clearly, the vectors in $\mathfrak{B}$ span $\mathcal{W}$. It is therefore enough to show that the vectors in $\mathfrak{B}$ are orthogonal. Let $S v_i$ and $S' v_j$ be two vectors in $\mathfrak{B}$ with $S = A^{j_0 ... j_{k-1}}_{i_0 ... i_{k-1}}$ and $S' = A^{j'_0 ... j'_{k-1}}_{i'_0 ... i'_{k-1}}$. We denote by $\mathcal{H}^{\text{B}}$ the Hilbert space of the qubits $i_0, ..., i_{k-1}$ and $i'_0, ..., i'_{k-1}$, and by $\mathcal{H}^{\text{A}}$ the Hilbert space of the rest of the qubits. Note that $\mathcal{H}^{\text{B}}$ consists of at most $2k$ qubits. Now, since V is $2k$-totally entangled subspace, it is maximally entangled relative to the decomposition $\mathcal{H} = \mathcal{H}^{\text{A}} \otimes \mathcal{H}^{\text{B}}$. Thus, from Proposition 5 we clearly have

$$\langle S v_i | S' v_j \rangle = \langle v_i | v_j \rangle \text{Tr}\left(\tilde{S}^\dagger \tilde{S}'\right) = \delta_{ij} \delta_{SS'} \ ,$$

where $S \equiv I^{\text{A}} \otimes \tilde{S}$ and $S' \equiv I^{\text{A}} \otimes \tilde{S}'$; that is, $\tilde{S}$ and $\tilde{S}'$ are the projections of S and S' onto $\mathcal{H}^{\text{B}}$, respectively. Hence, $\mathfrak{B}$ is an orthonormal basis of $\mathcal{W}$.

Since $\mathfrak{B}$ is an orthonormal basis we can construct an observable (i.e. Hermition operator) R such that for all $v \in V$ $R(Sv) = \lambda_S Sv$ with all of the λ_S distinct. We also define R to be zero on the orthogonal complement to $\mathcal{W}$ in $\mathcal{H}$. Now, suppose that an element v has been changed by a k-qubit transformation yielding $X_{i_0 ... i_{k-1}} v$. We do a measurment of R and since the image is in $\mathcal{W}$ the outcome is λ_S for some S. After the measurment, the quantum state is Sv and so we recover v by applying S^{-1} (actually S if we used the Pauli basis). The converse follows from the same lines in the opposite direction. This completes the proof. □

Note that Corollary 4 together with the proposition above is consistent with the quantum Singleton

bound [22], $n \geq 4k + l$, which also follows trivially from the quantum Hamming bound for the case of orthogonal codes that we considered in this subsection.

IV. SUMMERY AND CONCLUSIONS

We introduced the notion of entanglement of subspaces as a measure that quantify the entanglement of bipartite states in a randomly selected subspace. We discussed its properties and suggested that it is additive. We were not able to prove this conjecture (which is equivalent to the additivity conjecture of the entanglement of formation) although some numerical tests [14] supports that and for maximally entangled subspaces we proved that it is additive. We then extended the definition of maximally entangled subspaces into k-totally entangled subspaces and showed that the later can play an important role in the study of quantum error correction codes.

We considered both degenerate and non-degenerate codes and showed that the subspace spanned by the logical codewords of a non-degenerate code is a k-totally (maximally) entangled subspace. This observation, followed by an analysis of the degenerate Shor's nine qubits code in terms of 22 mutually orthogonal subspaces, motivated us to define a general (possible degenerate) error correcting code in terms of subspaces. We believe that further investigation in this direction would lead to a better understanding of degenerate quantum error correcting codes.

Acknowledgments:— The authors would like to thank Aram Harrow and David Meyer for fruitful discussions.

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] M. B. Plenio, S. Virmani, Quant. Inf. Comp. **7**, 1 (2007).
[4] P. W. Shor, Commun. Math. Phys. **246**, 453 (2004).
[5] G. Gour, Phys. Rev. A 72, 022323 (2005).
[6] P. Hayden, quant-ph/0409157
[7] P. Hayden, D. W. Leung and A. Winter, Comm. Math. Phys. **265**, 95 (2006).
[8] A. Abeyesinghe, P. Hayden, G. Smith and Andreas Winter, IEEE Trans. Inform. Theory **52**, 3635 (2006).
[9] P. Shor, Lecture Notes 2002, http://www.msri.org/ publications/ln/msri/2002/quantumcrypto/shor/1/
[10] N. R. Wallach, "An Unentangled Gleason's theorem", Quantum computation and information (Washington, DC, 2000), 291–298,Contemp. Math. 305(2002).
[11] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[12] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Comm. Math. Phys. **238**, 379 (2003).
[13] A. Roy and G. Gour, in preparation.
[14] A. W. Harrow, private communication.
[15] D. N. Page, Phys. Rev. Lett. **71**, 1291 (1993).
[16] G. Vidal, W. Dur and J. I. Cirac, Phys. Rev. Lett. 89, 027901 (2002).
[17] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information" (Cambridge University Press, 2000).
[18] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996); Proc. R. Soc. London A, **452**, 2551 (1996).
[19] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[20] R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[21] P. Shor, Phys. Rev. A **52**, 2493 (1995).
[22] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).